EXHIBIT A

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

IN RE SHIELDS HEALTH CARE GROUP, INC. DATA BREACH LITIGATION	Civil Action No. 22-10901

MEMORANDUM AND ORDER

March 5, 2024

Saris, D.J.

INTRODUCTION

Shields Health Care Group, Inc. provides medical scanning and surgical services to patients in over forty locations throughout the Northeast. In March 2022, hackers launched a cyber-attack on Shields's systems and gained access to the personally identifiable information and protected health information of an estimated two million patients. Plaintiffs are patients whose data was compromised during the breach. They bring this class action against Shields alleging twenty-one causes of action, seven of which they have voluntarily dismissed. Shields now moves to dismiss all remaining counts for failure to state a claim. After a hearing, the Court **ALLOWS IN PART** and **DENIES IN PART** Shields's motion (Dkt. 85).

BACKGROUND

Drawing all inferences in favor of Plaintiffs, the facts as alleged in the consolidated complaint are as follows. Shields is a health provider incorporated and principally doing business in Massachusetts. It operates more than forty facilities in New England as well as Maine, Maryland, Rhode Island, and New Hampshire. Shields facilities offer scanning and surgical services. In the course of its business, Shields collects and stores patients' private information. Shields's website includes a privacy policy stating that it would "[m]aintain the privacy of [patients'] health information as required by law." Dkt. 64 at 23. The privacy policy also "describes how [Shields] may use and disclose medical information for each category of uses or disclosures." Id.

On March 7, 2022, third-party criminal hackers breached Shields's computer systems. They maintained uninterrupted access until March 21, 2022, during which time they exfiltrated approximately two million patients' records, including patients' Social Security numbers, private health diagnoses, insurance data, and other highly sensitive information. Plaintiffs James Buechler,

Julie Colby, John Kennedy, Sharon Pimental, and Cindy Tapper are patients whose private information was compromised by the breach.[1]

It took until March 28, 2022 -- at least one week after the breach ended -- for Shields to become aware it had occurred. Shields did not begin alerting impacted patients until June 7, 2022, over two months later. Some patients, including Kennedy and Tapper, did not receive notice of the breach until late July 2022, nearly four months after Shields discovered it. See id. at 16, 21. Moreover, Shields's notice "fail[ed] to provide basic details" including "how unauthorized parties accessed [Shields's] computer server, whether the information was encrypted or otherwise protected, how [Shields] learned of the Data Breach, whether the Breach was a system-wide breach, whether servers storing information were accessed, and how many patients were affected by the Data Breach." Id. at 10-11. The notice also stated that Shields had "immediately launched an investigation into" the breach. Id. at 10.

As a result of the breach, Plaintiffs claim their private information "is now for sale to criminals on the dark web." Id. at 11. One named Plaintiff, Buechler, has experienced thousands of dollars in fraudulent bank charges and suspicious activity on his email account. He also purchased identity

[1] They are residents of Maryland, Maine, Rhode Island, Rhode Island, and New Hampshire, respectively.

protection that costs $299 per year. The other named Plaintiffs -- Colby, Kennedy, Pimental, and Tapper -- have neither suffered from actual fraud nor purchased protection services. However, they have experienced inconvenience and emotional distress due to the breach. Plaintiffs have spent time and energy monitoring their online accounts and anticipate needing to continue doing so because there is an ongoing risk their private information will be misused. Moreover, they claim the breach caused their private information to lose value.

At least thirty days prior to filing their complaint, Plaintiffs sent a Chapter 93A demand letter to Shields "identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered."[2] Id. at 84. On January 9, 2023, Plaintiffs filed a consolidated class complaint raising twenty-one claims: eleven common law claims on behalf of a putative nationwide class[3] and ten state-law claims by individual

[2] Plaintiffs did not attach their demand letter to the complaint but reference having sent it to Shields. See Dkt. 64 at 84. Defendants have appended the demand letter and seek to incorporate it by reference. See Dkt. 86 at 27 (citing Flores v. OneWest Bank, F.S.B., 886 F.3d 160, 167 (1st Cir. 2018)). Plaintiffs do not oppose introduction of the demand letter and the Court incorporates it by reference.

[3] Negligence (Count I), negligence per se (Count II), express and implied breach of contract (Counts III & IV), breach of the implied covenant of good faith and fair dealing (Count V), negligent misrepresentation (Count VI), invasion of privacy by intrusion (Count VII), breach of fiduciary duty (Count VIII), breach of confidence (Count IX), declaratory judgment (Count X), and unjust enrichment (Count XI).

named Plaintiffs on behalf of state-specific subclasses[4] (Dkt. 64). Shields moved to dismiss under Rule 12(b)(6) on August 23, 2023 (Dkt. 85). Plaintiffs voluntarily dismissed Counts II, IX, X, XIV, XVI, XVII, and XVIII. Dkt. 98 at 1 n.1. The Court held a hearing on Shields's motion on November 27, 2023.

LEGAL STANDARD

To survive a motion to dismiss, a complaint must allege "a plausible entitlement to relief." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 559 (2007). "While a complaint attacked by a Rule 12(b)(6) motion does not need detailed factual allegations, a plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions, and a formulaic recitation of a cause of action's elements will not do." Id. at 555 (citations and internal punctuation omitted); see also Rodriguez-Ortiz v. Margo Caribe, Inc., 490 F.3d 92, 95-96 (1st Cir. 2007). The plausibility standard requires the Court to proceed in two steps. First, the Court must "separate the complaint's

[4] Violations of the Rhode Island Deceptive Trade Practices Act (Count XII), Maine Unfair Trade Practices Act (Count XIII), Maine Uniform Deceptive Trade Practices Act (Count XIV), Maine Confidentiality of Health Care Information Law (Count XV), Maryland Consumer Protection Act (Count XVI), Maryland Personal Information Protection Act (Count XVII), Maryland Social Security Number Privacy Act (Count XVIII), New Hampshire Consumer Protection Act (Count XIX), New Hampshire Notice of Security Breach statute (Count XX), and Massachusetts Consumer Protection Act (Count XXI). Although labeled "Count XXII," the Massachusetts Consumer Protection Act claim is the twenty-first listed. Dkt. 64 at 82.

factual allegations (which must be accepted as true) from its conclusory legal allegations (which need not be credited)." Morales-Cruz v. Univ. of P.R., 676 F.3d 220, 224 (1st Cir. 2012). The Court must then determine whether the factual allegations permit it "to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)).

DISCUSSION

I. Negligence (Count I)

Plaintiffs claim that Shields negligently "fail[ed] to provide fair, reasonable, or adequate computer systems and data security practices" to protect Plaintiffs' private information. Dkt. 64 at 46. To state a claim for negligence, Plaintiffs must show "(1) a legal duty owed to the plaintiff[s] by the defendant; (2) a breach of that duty by the defendant; (3) causation; and (4) actual loss by the plaintiff[s]." Delaney v. Reynolds, 825 N.E.2d 554, 556 (Mass. App. Ct. 2005) (citing Glidden v. Maglio, 722 N.E.2d 971, 973 (Mass. 2000)).

Shields argues that the "economic loss doctrine" bars Plaintiffs' negligence claim. The economic loss doctrine prohibits recovery in tort "unless the plaintiffs can establish that the injuries they suffered due to the [defendant's] negligence involved physical harm or property damage, and not solely economic loss." Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918

N.E.2d 36, 46 (Mass. 2009) (holding in data breach case that "the costs of replacing credit cards for compromised accounts[] were economic losses" barred by the doctrine); see In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498-99 (1st Cir. 2009) (affirming dismissal of negligence claim in data breach case). "Massachusetts courts have declined to apply the economic loss doctrine to tort claims against a fiduciary." Szulik v. State St. Bank and Tr. Co., 935 F. Supp. 2d 240, 271 n.11 (D. Mass. 2013) (citing Clark v. Rowe, 701 N.E.2d 624, 626 (Mass. 1998)). Here, Plaintiffs have plausibly alleged that because Shields provided them healthcare, it was their fiduciary. See Alberts v. Devine, 479 N.E.2d 113, 120 (Mass. 1985) ("[T]he physician-patient relationship possesses fiduciary as well as contractual aspects." (citations omitted)); see also Tashjian v. CVS Pharmacy, Inc., No. 19-11164, 2020 WL 1931859, at *6-7 (D. Mass. Mar. 13, 2020) (recognizing a pharmacist-patient fiduciary relationship); Shedd v. Sturdy Mem'l Hosp., Inc., No. 2173CV00498C, 2022 WL 1102524, at *8 (Mass. Sup. Ct. Apr. 5, 2022) (declining to apply the economic loss doctrine in a data breach case involving the loss of private health information because there was a "special relationship" between hospital and patient). Thus, the economic loss doctrine does not provide a shield to Plaintiffs' negligence claim.

Alternatively, Shields parries that other than Buechler, Plaintiffs have not pleaded "actual loss" sufficient to support

their negligence claims. See Dkt. 64 at 14. Plaintiffs counter that they "are now at a heightened risk of exposure" because of the breach, and as a result, "must now and in the future closely monitor their financial accounts to guard against identity theft." Dkt. 64 at 4-5. They point out that some of Plaintiffs' private information has already been misused, indicating the risk they face is real, not hypothetical. See id. at 12 (alleging Buechler has already suffered fraud); id. at 15-23 (asserting that other Plaintiffs report an increase in suspicious calls from scammers and phishers). In light of an increase in suspicious activities, the confidential nature of the exposed health information, and the disclosure of Social Security numbers, Plaintiffs plausibly allege they will have to monitor their online accounts continually because of the ongoing risk of someone misusing their private information. Where Plaintiffs show a substantial risk of harm manifesting in the future, the "element of injury and damage will have been satisfied and the cost of that monitoring is recoverable in tort." Donovan v. Philip Morris USA, Inc., 914 N.E.2d 891, 901 (Mass. 2009); see Shedd, 2022 WL 1102524, at *6 (citing Donovan, 914 N.E.2d at 891); cf. Webb v. Injured Workers Pharmacy, LLC, No. 22-10797, 2023 WL 5938606, at *2 (D. Mass. Sept. 12, 2023) (holding that injuries including plaintiffs' "continued risk of harm due to the exposure and potential misuse of their personal data" constituted a "plausible case that plaintiffs were harmed" by the

data breach). Plaintiffs' negligence claim (Count I) is not dismissed insofar as they seek costs of present and future account monitoring.[5]

II. Express Contract (Count III)

Plaintiffs allege Shields breached its contractual duties by failing to secure their private information adequately. To state a claim for breach of contract under Massachusetts law, the plaintiff must allege "(1) a valid contract between the parties existed, (2) the plaintiff was ready, willing, and able to perform, (3) the defendant was in breach of the contract, and (4) the plaintiff sustained damages as a result." Omori v. Brandeis Univ., 635 F. Supp. 3d 47, 52 (D. Mass. 2022) (quoting In re Bos. Univ. COVID-19 Refund Litig., 511 F. Supp. 3d 20, 23 (D. Mass. 2021)).

Plaintiffs allege they entered "written agreements" with Shields as "part of the medical services [Shields] provided to Plaintiffs." Dkt. 64 at 48. Plaintiffs also allege that Shields's

[5] Plaintiffs Colby, Kennedy, Pimental, and Tapper also claim to have suffered garden-variety emotional distress and lost time. Although these harms are sufficient for Article III standing, see Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 376-78 (1st Cir. 2023), Massachusetts law is not settled on whether they suffice to state a claim for negligence, see Nancy P. v. D'Amato, 517 N.E.2d 824, 826 (Mass. 1988) ("[A] plaintiff may not recover for negligent infliction of emotional distress unless she has suffered physical harm."); Portier v. NEO Tech. Sols., No. 17-30111, 2019 WL 7946103, at *16 (D. Mass. Dec. 31, 2019) (noting that although "general allegations of lost time are too speculative to constitute cognizable injury," harms suffered mitigating effects of tortious conduct are normally compensable), report and recommendation adopted, 2020 WL 877035 (D. Mass. Jan. 30, 2020).

"failure to protect" Plaintiffs' private information "constitute[d] a material breach of the terms of these agreements." Id. Although Plaintiffs do not specify the terms of any written or oral agreements, they do reference Shields's online privacy statement, which affirmed Shields's responsibility to "[m]aintain the privacy of [patients'] health information as required by law" and described how Shields "may use and disclose medical information for each category of uses or disclosures." Id. at 23. Plaintiffs do not allege that they relied on or even read the privacy statement.

The legal question is whether a privacy statement on a website can create an express contract. Some courts have held that broad statements on a public-facing website, without more, are insufficient to form an express contract with users. See e.g., Delisle v. McKendree Univ., 73 F.4th 523, 527 (7th Cir. 2023) ("[M]arketing statements on a public-facing website are [not] terms of an express contract themselves . . . as they do not clearly demonstrate an intent to be bound." (cleaned up)); Doe v. Regents of Univ. of Cal., No. 23-00598, 2023 WL 3316766, at *6 (N.D. Cal. May 8, 2023); Gardner v. Health Net, Inc., No. 10-2140, 2010 WL 11597979, at *6 (C.D. Cal. Aug. 12, 2010) (citing Dyer v. Nw. Airlines Corp., 334 F. Supp. 2d 1196, 1199-200 (D.N.D. 2004)). In other contexts, courts have held that a defendant's online privacy statement constituted an enforceable contract because it

included a specific promise to use "reasonable . . . measures to protect" customers' personal data and a provision confirming assent by the user to its terms and conditions. In re Marriott Int'l, Inc., 440 F. Supp. 3d. 447, 482-84 (D. Md. 2020) (declining to dismiss breach of express contract claims in a data breach case). The complaint does not allege that Plaintiffs relied on the privacy statement or assented to any agreement incorporating a privacy protection. Therefore, Plaintiffs' breach of express contract claim (Count III) is dismissed.

III. Implied Contract (Count IV)

Plaintiffs claim Shields breached an implied contract by failing to safeguard their private information.

Under Massachusetts law, in "the absence of an express agreement, an implied contract may be inferred" from "the conduct of the parties" and "the relationship of the parties." T.F. v. B.L., 813 N.E.2d 1244, 1249 (Mass. 2004). To prove an implied-in-fact contract, Plaintiffs may rely on policy directives, employee handbooks, and corporate manuals as evidence of an implied-in-fact contract. Salvas v. Wal-Mart Stores, Inc., 893 N.E.2d 1187, 1211 (Mass. 2008). "A contract implied in fact requires the same elements as an express contract and differs only in the method of expressing mutual assent." Mass. Eye & Ear

Infirmary v. QLT Phototherapeutics, Inc., 412 F.3d 215, 230 (1st Cir. 2005) (citation omitted).

Courts have recognized that implied contract claims can be based on promises made in websites. See Omori, 635 F. Supp. 3d at 54-55 (holding that defendant's representations on its "website, brochures, admission materials, handbooks[,] and other publications" were evidence of "an implied contractual right"); Hickey v. Univ. of Pittsburgh, 81 F.4th 301, 311-12 (3d Cir. 2023) (citing McCabe v. Marywood Univ., 166 A.3d 1257, 1262 (Pa. Super. Ct. 2017)) (construing Pennsylvania law); Aubrey v. New Sch., 624 F. Supp. 3d 403, 417-18 (S.D.N.Y. 2022) (construing New York law). However, to support a claim for breach of an implied-in-fact contract, Plaintiffs must allege sufficient facts to permit an inference that the parties reciprocally agreed to enter into an agreement based on the online privacy statement. No such allegations are made.

Even in the absence of allegation of assent either expressly or by conduct, Plaintiffs can prevail if they demonstrate a contract implied in law. "A quasi contract or a contract implied in law is an obligation created by law 'for reasons of justice, without any expression of assent and sometimes even against a clear expression of dissent.'" Salamon v. Terra, 477 N.E.2d 1029, 1031 (Mass. 1985) (quoting 1 A. Corbin, Contracts § 19 (1963)). It is appropriate for the Court to find a contract implied in law when

"reasonable expectations" of the plaintiffs "are defeated." Liss v. Studeny, 879 N.E.2d 676, 682-83 (Mass. 2008) (citing Salamon, 477 N.E.2d at 1029).

Plaintiffs have plausibly shown that they had an implied-in-law contract with Shields to receive medical treatment in exchange for providing confidential health and financial information, which Shields was reasonably expected to keep private consistent with relevant data privacy laws. See Shedd, 2022 WL 1102524, at *10 (finding a plausible implied contract by healthcare provider to protect private information patients were required to disclose). Plaintiffs' expectations of data security were reasonable given the federal laws that govern handling private information. The so-called "HIPAA Security Rule" requires healthcare providers to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity" of private health information. 45 C.F.R. § 164.306(a)(2). Moreover, HIPAA requires notice of a breach implicating protected health information within sixty days of discovery. See Dkt. 64 at 2; 45 C.F.R. § 164.404(b). The Federal Trade Commission ("FTC") also requires that businesses accurately represent their data security policies to customers. See F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 245-46 (3d Cir. 2015). Thus, Plaintiffs have plausibly alleged that Shields violated

contractual obligations implied in law to protect their private medical information (Count IV).

IV. Implied Covenant of Good Faith and Fair Dealing (Count V)

Next, Plaintiffs claim Shields breached the implied covenant of good faith and fair dealing by not faithfully "carrying out its contractual obligations" to protect their private information according to relevant laws, regulations, and industry standards. Dkt. 64 at 50. All contracts in Massachusetts are "subject to an implied covenant of good faith and fair dealing." Robert & Ardis James Found. v. Meyers, 48 N.E.3d 442, 449 (Mass. 2016). It provides that "neither party shall do anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract." Druker v. Roland Wm. Jutras Assocs., Inc., 348 N.E.2d 763, 765 (Mass. 1976) (quoting Uproar Co. v. Nat'l Broad. Co., 81 F.2d 373, 377 (1st Cir. 1936)). To state a claim for a breach of the covenant of good faith and fair dealing, the plaintiff must show that the defendant "violate[d] [its] reasonable expectations," Chokel v. Genzyme Corp., 867 N.E.2d 325, 329 (Mass. 2007), and performed with a "lack of good faith," T.W. Nickerson, Inc. v. Fleet Nat'l Bank, 924 N.E.2d 696, 704 (Mass. 2010).

Plaintiffs have alleged that Shields acted with a "lack of good faith" by taking "three to four months" to notify patients of the breach, Dkt. 98 at 26, and by eventually providing notice that

did not adequately describe the breach's causes and scope, see Dkt. 64 at 10-11; Zoll Med. Corp. v. Barracuda Networks, Inc., 585 F. Supp. 3d 128, 138 (D. Mass. 2022). Thus, Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing (Count V) is not dismissed.

V. Negligent Misrepresentation (Count VI)

Plaintiffs claim that Shields "negligently and recklessly misrepresented material facts" by "representing that [it] did and would comply" with data privacy laws. Dkt. 64 at 52. To state a claim of negligent misrepresentation, the plaintiff must show that:

> [T]he defendant, (1) in the course of [its] business . . . (2) supplied false information for the guidance of others (3) in their business transactions, (4) causing and resulting in pecuniary loss to those others (5) by their justifiable reliance on the information, and that she (6) failed to exercise reasonable care or competence in obtaining or communicating the information.

See DeWolfe v. Hingham Ctr., Ltd., 985 N.E.2d 1187, 1192 (Mass. 2013). Plaintiffs state a plausible claim that Shields "supplied false information" by representing that it would "[m]aintain the privacy of [their] health information as required by law." Dkt. 64 at 23. However, Plaintiffs have not alleged that they read the privacy statement or relied on it. The complaint alleges in conclusory form that Plaintiffs relied on misrepresentations by Shields but does not state with specificity what misrepresentations they relied on. See Dkt. 64 at 52. The only

misrepresentations inferred in the complaint were those contained in the privacy statement. The claim is dismissed.

VI. Invasion of Privacy by Intrusion (Count VII)

Plaintiffs allege that by "fail[ing] to protect and safeguard" their private information, Shields "intruded on the[ir] private and personal affairs." Dkt. 64 at 53. Massachusetts General Laws Chapter 214, § 1B creates an actionable "right against 'unreasonable, substantial or serious' interference with a person's privacy." Ayash v. Dana-Farber Cancer Inst., 822 N.E.2d 667, 681 (Mass. 2005) (quoting Mass. Gen. Laws ch. 214, § 1B). To succeed on a claim under the statute, a plaintiff must show there was a "gathering and dissemination of privation information" by the defendant. Nelson v. Salem State Coll., 845 N.E.2d 338, 348 (Mass. 2006). Some courts have held invasion of privacy "is an intentional tort under Massachusetts law." Elliott-Lewis v. Lab'ys, 378 F. Supp. 3d 67, 71 (D. Mass. 2019).

Plaintiffs' claim does not pass muster because Plaintiffs allege only that hackers disseminated their private information and intruded on their privacy, not that Shields did. See Webb, 2023 WL 5938606, at *5 (dismissing invasion of privacy claim for plaintiff's "fail[ure] to allege any intentional acts on the part of" the defendant "that could be said to have been the legal cause"

of the data breach). Accordingly, Plaintiffs' claim for invasion of privacy (Count VII) is dismissed.

VII. Breach of Fiduciary Duty (Count VIII)

Plaintiffs allege that Shields breached its fiduciary duty of confidentiality by failing to implement proper data security protocols, to timely notify them of the breach, and to investigate the breach adequately. To state a claim for breach of fiduciary duty under Massachusetts law, Plaintiffs must show "(1) the existence of a duty of a fiduciary nature, based upon the relationship of the parties, (2) breach of that duty, and (3) a causal relationship between that breach and some resulting harm to the plaintiff." Amorim Holding Financeria, S.G.P.S., S.A. v. C.P. Baker & Co., 53 F. Supp. 3d 279, 295 (D. Mass. 2014) (quoting Hanover Ins. Co. v. Sutton, 705 N.E.2d 279, 288–89 (Mass. App. Ct. 1999)).

Plaintiffs have adequately pleaded that as their healthcare provider, Shields was their fiduciary. See Alberts, 479 N.E.2d at 120 ("[T]he physician-patient relationship possesses fiduciary as well as contractual aspects." (citations omitted)); Tashjian, 2020 WL 1931859, at *6-7. Plaintiffs have alleged that they were "dependent on [Shields]'s judgment" to protect their private information. UBS Fin. Servs., Inc. v. Aliberti, 133 N.E.3d 277, 288 (Mass. 2019). Shields required them to provide private information and represented it would "[m]aintain the privacy of

[Plaintiffs'] health information as required by law." Dkt. 64 at 23. That is sufficient to allege that Shields owed them a fiduciary duty to protect their private information, and to provide prompt notification and a reasonable investigation of any breach. Thus, Plaintiffs' fiduciary duty claim (Count VIII) is not dismissed.

VIII. Unjust Enrichment (Count XI)

Plaintiffs allege that Shields unjustly enriched itself by accepting reimbursement for treatment but not using it "to pay for the administrative costs of reasonable data privacy and security." Dkt. 64 at 62. Under Massachusetts law, "[u]njust enrichment is defined as retention of money or property of another against the fundamental principles of justice or equity and good conscience." Sacks v. Dissinger, 178 N.E.3d 388, 397 (Mass. 2021) (quoting Santagate v. Tower, 833 N.E.2d 171, 176 (Mass. App. Ct. 2005)). To state a claim, a plaintiff "must show (1) a benefit conferred upon defendant by plaintiff, (2) an appreciation or knowledge by defendant of the benefit, and (3) that acceptance or retention of the benefit under the circumstances would be inequitable without payment for its value." Infinity Fluids Corp. v. Gen. Dynamics Land Sys., Inc., 210 F. Supp. 3d 294, 309 (D. Mass. 2016). Whether a benefit is "unjust" turns "on the reasonable expectations of the parties." Metro. Life Ins. Co. v. Cotter, 984 N.E.2d 835, 850 (Mass. 2013). And "[a]lthough damages for breach of contract and

unjust enrichment are mutually exclusive," a plaintiff may plead them in the alternative. Chang v. Winklevoss, 123 N.E.3d 204, 212 (Mass. App. Ct. 2019). The Court will not dismiss this count as an alternative theory of relief.

IX. Rhode Island Deceptive Trade Practices Act (Count XII)

On behalf of the Rhode Island Sub-Class, Kennedy and Pimental raise claims under the Rhode Island Deceptive Trade Practices Act ("RIDTPA"). The RIDTPA declares unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." R.I Gen. Laws § 6-13.1-2. The statute's safe-harbor exemption states that the statute "shall [not] apply to actions or transactions permitted under laws administered by the department of business regulation or other regulatory body or officer acting under statutory authority of this state or the United States." Id. § 6-13.1-4.

The Supreme Court of Rhode Island analyzes the statutory safe harbor using a two-step burden-shifting framework. First, the party invoking the safe harbor exemption must "demonstrate that the general activities complained of are subject to monitoring or regulation by a state or federal government agency." Lynch v. Conley, 853 A.2d 1212, 1214 (R.I. 2004). Here, as Shields notes, Plaintiffs allege that Shields is liable under the RIDTPA specifically because it "failed to comply with its obligations to protect and secure the Private Information under HIPAA . . . and

the FTCA." Dkt. 64 at 63-64. Thus, the burden shifts to Plaintiffs to show that "the specific acts at issue are not covered by the exemption." Lynch, 853 A.2d at 1214 (quoting State v. Piedmont Funding Corp., 382 A.2d 819, 822 (R.I. 1978)). Plaintiffs have not done so. See Dkt. 98 at 34 (stating in conclusory fashion that "neither the FTC Act . . . nor HIPAA . . . were promulgated or enforced to regulate the specific conduct challenged here"). Thus, their claim under the RIDTPA (Count XII) is dismissed.

X. Maine Unfair Trade Practices Act (Count XIII)

On behalf of the Maine Sub-Class, Colby raises claims under the Maine Unfair Trade Practices Act ("MUTPA"). The MUTPA prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Me. Rev. Stat. Ann. tit. 5, § 207. Maine courts have held that the MUTPA only allows for a private cause of action when the plaintiff has suffered a "substantial loss" of "money or property." See Anderson v. Hannaford Bros. Co., 659 F.3d 151, 160 (1st Cir. 2011) (citing McKinnon v. Honeywell Int'l, Inc., 977 A.2d 420, 427 (Me. 2009)). Here, Colby alleges that the breach caused her to experience emotional distress, at least one suspected spam call, and lost time. But Maine courts do not allow plaintiffs to recover for lost time or emotional distress under the MUTPA. In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 660 F. Supp. 2d 94, 102 (D. Me. 2009) (quoting Bartner v. Carter, 405 A.2d 194, 203 (Me.

1979)). And even accepting that Colby received one or more spam calls, those do not constitute a substantial loss of money or property, nor do they constitute "substantial" injury. Accordingly, Plaintiffs' claim under the MUTPA (Count XIII) is dismissed.

XI. Maine Confidentiality of Health Care Information Law (Count XV)

On behalf of the Maine Sub-Class, Colby also raises claims under the Maine Confidentiality of Health Care Information Law ("MCHCIL"), which prohibits unauthorized disclosure of health care information. Me. Rev. Stat. Ann. tit. 22, § 1711-C(2). Disclosure is defined as "release, transfer of or provision of access to health care information in any manner obtained as a result of a professional health care relationship." Id. § 1711-C(1)(B). Because the complaint does not allege that Shields itself released, transferred, or provisioned access to Plaintiffs' private information, Plaintiffs have not sufficiently pled a violation of the MCHCIL. Instead, the complaint acknowledges that the breach involved "unauthorized" access to Plaintiffs' data. Dkt. 64 at 3. Furthermore, the MCHCIL only allows private action against persons who "intentionally unlawfully disclosed health care information." Me. Rev. Stat. Ann. tit. 22, § 1711-C(13)(B). Here, Plaintiffs have not plausibly alleged that Shields acted with intent to

disclose their private information. As a result, Plaintiffs' MCHCIL claim (Count XV) fails.

XII. New Hampshire Consumer Protection Act (Count XIX)

On behalf of the New Hampshire Sub-Class, Tapper raises claims under the New Hampshire Consumer Protection Act ("NHCPA"). The NHCPA forbids practices that include "[r]epresenting that goods or services have . . . characteristics . . . that they do not have," or that they "are of a particular standard, quality, or grade . . . if they are of another." N.H. Rev. Stat. Ann. §§ 358-A:2(V)-(VII). It also prohibits "[a]dvertising goods or services with intent not to sell them as advertised." Id. § 358-A:2(IX).

Tapper alleges that Shields "[f]ail[ed] to implement and maintain appropriate and reasonable security procedures and practices" to protect private information, and to disclose that its "data security practices were inadequate to safeguard and protect" Plaintiffs' private information, which according to Tapper constituted an unfair or deceptive trade practice. Dkt. 64 at 79.[6] Tapper also claims that Shields unlawfully misrepresented the quality of its data security by stating on its website that it "[m]aintain[s] the privacy of [patients'] health information as required by law" and "takes the confidentiality,

[6] Tapper also alleges that Shields "[f]ail[ed] to disclose" the breach "as soon as possible," violating N.H. Rev. Stat. Ann. § 359-C:20(I)(a). Dkt. 64 at 79. Count XX covers Tapper's claims under that statute.

privacy, and security of information in [its] care seriously." Dkt. 64 at 23, 78-79. Shields responds that the NHCPA does not cover a "fail[ure] to maintain and implement adequate data security procedures" and that the complaint does not allege Shields "ever represented it had particular data security practices or procedures." Dkt. 86 at 25.

In an analogous case, a district court held that plaintiffs had stated a claim under NHCPA by alleging that the defendant had "affirmatively represented that it would take 'reasonable security measures' to protect Plaintiffs' Personal Information" despite knowing its security was inadequate. See In re Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 1002 (S.D. Cal. 2014) (dismissing plaintiffs' claims on other grounds). Here, Plaintiffs allege that Shields's websites affirmatively stated that Shields "[m]aintain[s] the privacy of [patients'] health information as required by law" when it was not doing so. Dkt. 64 at 23. As a result, Tapper has stated a claim under the NHCPA.

XIII. New Hampshire Notice of Security Breach Statute (Count XX)

On behalf of the New Hampshire Sub-Class, Tapper also brings a claim under the New Hampshire Notice of Security Breach statute ("N.H. NSB"). The N.H. NSB requires that if an entity whose business involves collecting personal information "becomes aware of a security breach," it must "promptly determine the likelihood

that the information has been or will be misused." N.H. Stat. Rev. Ann. § 359-C:20(I)(a). If the entity determines that "misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made," the entity must "notify the affected individuals as soon as possible." Id. (emphasis added).

Tapper alleges that Shields knew of the breach by March 28, 2022, but did not inform her until July 26, 2022 -- nearly four months later -- which was not "as soon as possible." Dkt. 64 at 21, 81. Shields responds that it "immediately launched an investigation" into the breach as required by the N.H. NSB, id. at 10, and that "[t]he Complaint is devoid of any allegations as to why the approximately three months was an unreasonable period to investigate the [i]ncident," Dkt. 86 at 26.

The New Hampshire statute imposes requirements similar to other state statutes "requir[ing] companies to notify individuals of data breaches without unreasonable delay." In re Arthur J. Gallagher Data Breach Litig., 631 F. Supp. 3d 573, 589 (N.D. Ill. 2022). Courts interpreting statutes with similar language have not dismissed claims where the defendant waited nine months, see id. at 590 (analyzing New Hampshire, California, Illinois, Louisiana, Maryland, and Colorado statutes), five months, see In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig., 613 F. Supp. 3d 1284, 1300 (S.D. Cal. 2020) (analyzing California statute), and four months, see In re Cap. One Consumer Data Sec. Breach Litig.,

488 F. Supp. 3d 374, 416-18 (E.D. Va. 2020) (analyzing Virginia and Washington statutes), to notify plaintiffs of a data breach. Thus, Tapper has stated a claim under the New Hampshire notice statute.

XIV. Massachusetts Consumer Protection Act (Count XXI)

Finally, Plaintiffs allege that by failing to keep their private information safe and to timely notify them of the breach, Shields violated the Massachusetts Consumer Protection Act ("MCPA"). Chapter 93A of the MCPA forbids "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Mass. Gen. Laws ch. 93A, § 2(a). Chapter 93H requires entities that own or license consumers' personal information to follow state and federal regulations governing data privacy and security measures, as well as to provide notice "as soon as practicable and without unreasonable delay" in the event of a suspected data breach. Id. ch. 93H, §§ 2-3.

To bring a claim under Chapter 93A, a plaintiff must first send the defendant "a written demand for relief, identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered." Id. ch. 93A, § 9(3). The demand letter is a "prerequisite to suit," Spring v. Geriatric Auth. of Holyoke, 475 N.E.2d 727, 735 (Mass. 1985), and "must describe the complained-of-acts with reasonable specificity," Delcid v. Am. Servicing Co., No. 11-11122, 2011 WL 5884274, at *1

(D. Mass. Oct. 3, 2011) (quoting Smith v. Jenkins, 777 F. Supp. 2d 264, 267 (D. Mass. 2011)). Shields argues that Plaintiffs' demand letter is "insufficient under the [MCPA]" because it "does not name the 'claimant(s),' as required" and "does not identify any alleged injuries." Dkt. 86 at 27-28. Plaintiffs counter that their demand letter was sufficiently specific to pass muster. See Dkt. 87-1.

Plaintiffs' demand letter sufficiently identifies the "claimant(s)" in this case. Shields argues that the demand letter fails to state "which Plaintiffs would be in the forthcoming consolidated class action complaint," including named Plaintiffs Kennedy, Pimental, and Tapper. Dkt. 86 at 27-28. However, "in a putative class action, the demand letter need only be sent by a class representative on behalf of herself and the entire class, as long as the letter sufficiently describes the claimant's injuries." Bosque v. Wells Fargo Bank, N.A., 762 F. Supp. 2d 342, 354 (D. Mass. 2011) (citing Baldassari v. Pub. Fin. Tr., 337 N.E.2d 701, 707 (Mass. 1975)); see also Hermida v. Archstone, 950 F. Supp. 2d 298, 305 (D. Mass. 2013). Here, the letter states that Plaintiffs intended to file suit "on behalf of themselves, any other individuals identified through ongoing investigation and discovery, and all absent putative class members." Dkt. 87-1 at 2.

The demand letter also sufficiently identifies the injuries Plaintiffs suffered. In the class context, the demand letter need

only describe "the individual claimant's own injury" because early in litigation, "both the size of the eventual plaintiff class . . . and the total extent of their eventually claimed damages [are] unknown and could not possibly be estimated." Richards v. Arteva Specialties S.A.R.L., 850 N.E.2d 1068, 1075 (Mass. App. Ct. 2006), rev. denied, 854 N.E.2d 441 (Mass. 2006) (table decision).

ORDER

For the reasons stated above, Shields's Motion to Dismiss (Dkt. 85) is **ALLOWED IN PART** as to Counts III (Express Contract), VI (Negligent Misrepresentation), VII (Invasion of Privacy), XII (Rhode Island Deceptive Trade Practices Act), XIII (Maine Unfair Trade Practices Act), and XV (Maine Confidentiality of Health Care Information Law), and **DENIED IN PART** as to Counts I (Negligence), IV (Implied Contract), V (Implied Covenant of Good Faith and Fair Dealing), VIII (Fiduciary Duty), XI (Unjust Enrichment), XIX (New Hampshire Consumer Protection Act), XX (New Hampshire Notice of Security Breach statute), and XXI (Massachusetts Consumer Protection Act).[7]

SO ORDERED.

/s/ PATTI B. SARIS
Patti B. Saris
United States District Judge

[7] As noted above, the complaint erroneously lists Plaintiffs' MCPA claim as "Count XXII." Dkt. 64 at 82.